REMARKS

This Amendment is in response to the Office Action mailed October 17, 2006. In the Office Action, claims 1-19 were rejected under 35 U.S.C. § 103. Reconsideration in light of the amendments and remarks made herein is respectfully requested.

Request for Examiner's Interview

The Examiner is respectfully requested to contact the undersigned attorney if after review, such claims are still not in condition for allowance. This telephone conference would greatly facilitate the examination of the present application. The undersigned attorney can be reached at the telephone number listed below.

Rejection Under 35 U.S.C. § 103

Claims 1-19 were rejected under 35 U.S.C. §103(a) as being unpatentable over Proudler (U.S. Patent Publication No. 2003/0226031 A1) in view of Ober (U.S. Patent No. 6,959,086). Applicant traverses the rejection because a *prima facie* case of obviousness has not been established.

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. *See MPEP §2143; see also In Re Fine, 873 F. 2d 1071, 5 U.S.P.Q.2D 1596 (Fed. Cir. 1988).* Herein, the combined teachings of the cited references fail to describe or suggest all the claim limitations.

With respect to independent claim 1, Applicant respectfully submits that neither Proudler nor Ober, alone or in combination, suggest the operation of performing a direct proof by the platform to prove that the platform possesses the cryptographic information. As claimed, the direct proof comprises a *plurality of exponentiations* each being conducted using an exponent having a bit length no more than one-half a bit length of a modulus (n). *Emphasis added.* Herein, paragraphs [0065-0066] of Proudler fail to provide any description of a direct proof technique as claimed and any alleged "direct proof" does not comprise the plurality of exponentiations as claimed.

Moreover, Ober is directed to key management and the selection of the bit length of a key (block 4 of FIG. 1) does not describe or suggest alteration of the exponent of the exponentiations forming the direct proof as claimed.

As another example, referring to claim 6, the Office Action is devoid of these exponentiations being conducted of the form $h^f \bmod P$ as claimed. Rather, the Office Action suggests that e mod ((p-1)(q-1)) provides such teachings. However, e ($\geq$65537) does not

constitute "h^t_x," where "t" is randomly chosen. Moreover, there is no teaching that ((p-1)(q-1)) constitutes a "prime number" (P) as claimed.

Since the same arguments applied to claim 1 can be further applied to independent claims 13 and 17, Applicant respectfully requests that the Examiner withdraw the rejection of claims 1-19 under 35 U.S.C. § 103(a) as being unpatentable over Proudler in view of Ober.

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.